Australian Government

Australia's Digital ID System

Consultation guide: Proposed amendments to the Digital ID Rules and the Digital ID (Accreditation) Rules

September - October 2025 public consultation

Department of Finance

Department of Finance is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, please contact the digital ID communications team at digitalid.communications@finance.gov.au.

Contents

Introduction

Australia's Digital ID System

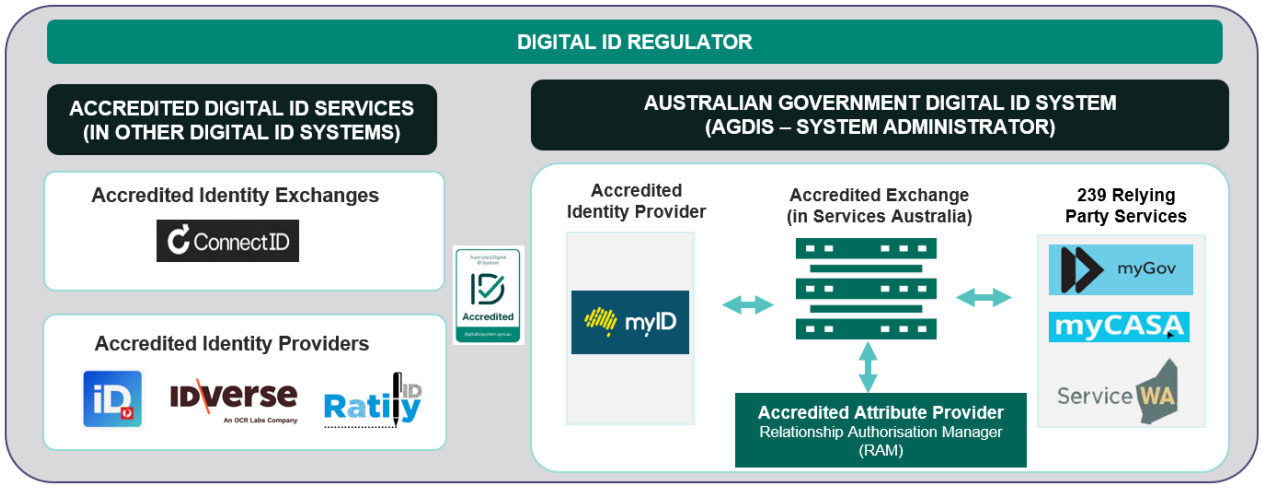
Australia's Digital ID System provides a secure, convenient and voluntary way for individuals to verify their identity and other things about themselves online.

Australia's Digital ID System is designed to promote the use of Digital ID services within government and across the broader economy through:

- an **Accreditation Scheme** that is open to providers of Digital ID services (i.e. Identity, Attribute or Exchange service providers) across the public and private sectors.
    - Accreditation demonstrates to consumers and business that the providers comply with privacy, security and other standards and safeguards.
    - Accredited providers can display the digital ID trustmark.
- the **Australian Government Digital ID System** which facilitates the use of Digital ID services that are provided by, or used by, government agencies.
    - From 30 November 2026, private sector entities will be able to apply to participate in the Australian Government Digital ID System as users of Digital ID services (participating relying parties) or as accredited providers of Digital ID services.

Australia's Digital ID System is illustrated in the diagram below.

Australia's Digital ID System



The Digital ID System regulators, administrator and independent technical standards authority are:

- the Australian Competition and Consumer Commission (**ACCC**) as the independent Digital ID Regulator, overseeing the Digital ID Accreditation Scheme and governance of the Australian Government Digital ID System (site for Digital ID Regulator)
- the Office of the System Administrator, overseeing the day-to-day operation of the Australian Government Digital ID System (site for System Administrator)
- the Office of the Australian Information Commissioner, who is the independent privacy regulator for accredited Digital ID services (site for OAIC)
- the Digital ID Data Standards Chair who makes technical and data standards (site for the Data Standards Chair | Data Standards Body).

You can find more information about the Digital ID System, the Australian Government Digital ID System and the Accreditation Scheme at https://www.digitalidsystem.gov.au/.

Digital ID Act 2024

The *Digital ID Act 2024* (**Digital ID Act**), *Digital ID Rules 2024* (**Digital ID Rules**), and *Digital ID (Accreditation) Rules 2024* (**Accreditation Rules**) commenced on 30 November 2024.

This legislation governs Australia's Digital ID System (**Digital ID System**), including the Accreditation Scheme and the Australian Government Digital ID System.

This public consultation is about proposed amendments to Digital ID Rules and the Accreditation Rules.

Using this guide

This guide is not intended to be an exhaustive description of the content of the proposed draft rules and standards. Details have been necessarily simplified or omitted. We recommend you read it alongside the source documents available at DigitalIDSystem.gov.au/have-your-say, which remain the authoritative description on the proposed laws.

Where to find more information

To help you understand more about the legislation, we recommend reading the source documents and resources that can be found on consultation page at DigitalIDSystem.gov.au.

Having your say

Consultation purpose

Your views are sought on the Exposure Drafts of:

- *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025*
- *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025*.

Your views will help refine the proposed amendments. If you wish to provide a submission, please read this guide.

Providing feedback

The consultation period will open on Thursday 18 September 2025 AEST and close at 5pm, Friday 17 October 2025 AEDT. Details on how to provide your feedback are available at DigitalIDSystem.gov.au/have-your-say, including an optional feedback template that is available for your use.

Consultation timeline

Step	Estimated Timeframe
This public consultation opens	**Thursday 18 September 2025**
This public consultation closes	**Friday 17 October 2025, 5pm AEDT**
Amending rules intended to commence	**By 30 November 2025**

Proposed changes to the Digital ID Rules

This section details the proposed changes contained in the *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025* (**Digital ID Amendment Rules**).

The Digital ID Amendment Rules amend the Digital ID Rules to:

1. Establish a redress framework for incidents that occur in relation to accredited services of accredited entities that are provided within the Australian Government Digital ID System.
2. Provide a framework for the System Administrator to direct entities to undertake investigation of incidents in certain circumstances and provide procedures for the conduct of that investigation.
3. Establish a streamlined application for approval to participate for state, territory and Commonwealth government participating relying parties that are affected by machinery of government changes.
4. Authorise the Digital ID Data Standards Chair to use the digital ID trustmark.

Redress framework for the Australian Government Digital ID System

The Digital ID Act requires that, within 12 months of the commencement of the Digital ID Act,[1] the Digital ID Rules must provide for a redress framework for incidents that occur in relation to services provided by approved entities within the Australian Government Digital ID System, and specifies the mandatory matters to be dealt with in that framework.[2]

The proposed redress framework is focussed on supporting individuals who are adversely affected by digital ID fraud and cyber security incidents within the Australian Government Digital ID System.

The proposed new redress mechanisms will bolster the existing requirements relating to the remediation of incidents and providing support to individuals, which are captured in the current rules, especially the Accreditation Rules.

The proposed changes are intended to:

1. improve the support for individuals who have been impacted by fraud and cybersecurity while using the Australian Government Digital ID System

[1] Digital ID Act, s 88(1).
[2] Digital ID Act, s 88(2).

2. effectively remediate digital IDs which have been subject to fraud or cybersecurity incidents
3. promote accountability of accredited entities and provide individuals with greater confidence
4. improve inefficiencies and regulatory oversight within the Australian Government Digital ID System.

Proposed requirement 1: Obligation to consider notification to affected individual

Currently, Identity Service Providers and Attribute Service Providers participating in the Australian Government Digital ID System are not required to contact or notify an individual impacted by a cyber security incident or digital ID fraud incident.

The proposed amendments will require entities to consider whether it is appropriate to notify an individual affected by a cyber security or digital ID fraud incident. In making this assessment, entities will be required to take into account factors such as:

- the likelihood of harm to the individual, and
- the potential impact on the operation of the Australian Government Digital ID System.

This approach aims to balance the need to inform individuals, so they can take steps to protect themselves, with the risk that notification could cause further harm, for example, by inadvertently assisting malicious actors.

The amendment promotes accountability by requiring entities to actively consider the impact on affected individuals, ensuring they are not overlooked in the response to an incident.

Proposed requirement 2: Obligation to publish policies relating to the identification, management and resolution of incidents

Currently, Identity Service Providers and Attribute Service Providers participating in the Australian Government Digital ID System are not required to publish policies relating to the identification, management and resolution of incidents. As a result, individuals affected by an incident may not understand how their data will be protected or what steps the entity will take to respond.

The amendments introduce a clear obligation on entities to publish policies that explain how they identify, manage, and resolve cyber security and digital ID fraud incidents. This ensures that this information is available to the public.

This reform promotes transparency and accountability, helping individuals understand how their data will be safeguarded and increasing public confidence in the Digital ID System.

Proposed requirement 3: Obligation to develop and publish complaint handling policies

Currently, Identity Service Providers and Attribute Service Providers participating in the Australian Government Digital ID System are not required to publish complaints procedures. As a result, individuals affected by an incident may not understand how to raise or resolve a complaint with the relevant entity.

The amendments will require entities to develop and publish clear complaints policies for individuals affected by digital ID fraud and cyber security incidents. The policies must outline how to make a complaint, how complaints will be handled, and the expected timeframes for resolution.

The policies do not need to be separate from other complaints handling policies that the entity uses for its other services.

This reform ensures individuals know how to make a complaint if something goes wrong and what to expect if they make a complaint, promoting fairness, accountability, and trust in the Australian Government Digital ID System.

Proposed requirement 4: Obligation to refer unresolved user issues to the System Administrator

Currently, Identity Service Providers and Attribute Service Providers participating in the Australian Government Digital ID System can escalate user issues to the System Administrator when they are unable to resolve the matter, if it relates to other services in the system. The System Administrator does not accept escalations or enquiries directly from individuals.

The amendments will require entities to refer unresolved technical issues to the System Administrator, including those that do not involve other services in the system. This change formalises existing guidance by embedding it in the rules.

Referrals must be made as soon as reasonably practicable. If the issue was raised through a complaint, the referral must occur within 28 days.

Before making a referral, the entity must be reasonably satisfied that the issue cannot be resolved without the referral. The entity must also assist the individual by directing them to relevant public resources or helping them contact another responsible entity.

The System Administrator may recommend a course of action for the entity, such as providing an explanation or issuing an apology.

This reform ensures that individuals are not left without a pathway to resolution, strengthening accountability and reinforcing confidence in the system's ability to respond to complex or unresolved issues.

Consultation questions for the redress framework:

1. Considering whether it is appropriate to notify an individual: *do the proposed factors to consider in relation to whether it is appropriate to notify an individual strike the right balance between user protection and security risks?*

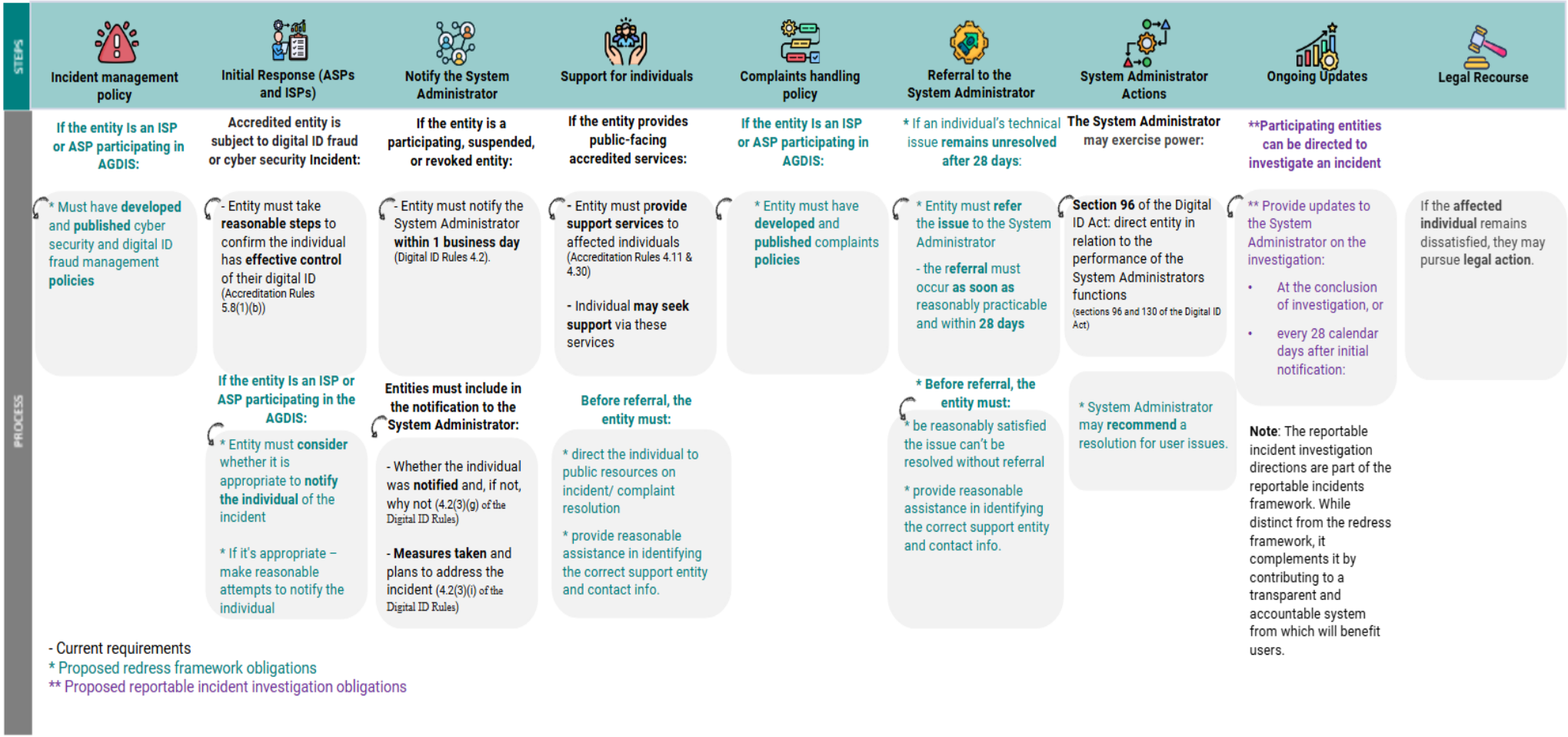
2. Published incidents policies: *are there any minimum requirements that the policies relating to the identification, management and resolution of incidents should contain, that would not exacerbate harm?*

3. Published complaints handling policies*: are the minimum requirements for the complaints policies satisfactory?*

4. Escalation to the System Administrator*: is the proposed escalation timeframe (within 28 days) sufficient to ensure timely resolution of unresolved user issues?*

Redress framework current and future state

Digital ID Fraud and Cybersecurity Incident Response Process (Australian Government Digital ID System)



Practical example

User Journey: Digital ID fraud incident

Name: Steph
Age: 28 years old
Scenario:
Steph is attempting to create a digital ID but is unable to verify her identity documents.

Application of proposed new redress requirements	
1. Requirement for ISPs and ASPs to consider whether it is appropriate to notify an affected individual. (4A.2)	Yes – applied to this scenario. ISP assessed and notified Steph
2. Requirement for ISPs and ASPs participating in the AGDIS to develop and publish complaints policies. (4A.8)	Yes – applied to this scenario ISP has a published complaints policy available to Steph.
3. Requirement for ISPs and ASPs participating in the AGDIS to escalate unresolved user issues to the OSA. (4A.3)	No. Not applicable to this scenario. The Digital IDs are suspended and therefore the user issue is resolved.

Application of proposed reportable obligations	
Requirement for entities who receive an information disclosure from the OSA to provide updates on the progress of their investigation every 28 days or at the conclusion of the investigation. (4.2(9))	Yes – applied to this scenario. PRP 1 concluded its investigation in 23 days; PRP 2 took 45 days and provided updates at 28 and 45 days

Steph attempted to create a digital ID through an Identity Service Provider (ISP) but was unable to verify her identity documents.

Concerned, Steph contacted the ISP's support channel and provided her trusted contact details. The support team escalated the issue to the ISP's investigation team.

The ISP identified that two digital IDs had been created in Steph's name, neither of which Steph had initiated.

The ISP contacted Steph using the trusted contact details and confirmed the fraud. The ISP suspended both digital IDs and provided Steph with remediation and support, including:

- Guidance on creating a new digital ID using alternative documents and a secure email address.
- Recommendations to report the incident to police, financial institutions, superannuation funds, and relevant government agencies.

Within 1 business day, the ISP notified the System Administrator via the Portal, in accordance with rule 4.2 of the Digital ID Rules 2024.

The Portal is a secure online platform used by accredited entities to report incidents and communicate with the System Administrator.

The notification included confirmation that Steph had been contacted and that an investigation was underway (paragraph 4.2(3)(g)).

The System Administrator investigated and discovered that the fraudulent digital IDs had interacted with two PRPs.

The System Administrator issued information disclosures to the PRPs, including Steph's trusted contact details, under APP 6.2(e) and the Data Sharing Principles.

An information disclosure allows the System Administrator to share incident details with other affected entities so they can investigate and support the individual.

Having determined it appropriate to do so, the ISP formally notified Steph that the incident constituted digital ID fraud, in accordance with new rule 4A.2.

Steph was provided with public resources and support under new rule 4A.5, including information about the ISP's complaints process.

During this time, PRPs continued to provide services to Steph using alternate identity verification methods under section 74 of the Digital ID Act.

The PRPs commenced investigations promptly:

- PRP 1 concluded its investigation in 23 days.
- PRP 2 took 45 days to complete its investigation and provided updates at 28 and 45 days, in accordance with rule 4.2(9).

Participating Relying Party PRP- A service provider that uses verified personal information from an accredited source to offer or enable access to services.
Identity Service Provider ISP- Generates, manages, maintains or verifies information about the identity of an individual to create or manage a digital ID
Attribute Service Provider ASP- Verifies and manages attributes, which are additional pieces of information that can be associated with a person's digital identity
Entity- Identity Service Providers, Attribute Service Providers, Identity Exchange Providers, Participating Relying Party
AGDIS- Australian Government Digital ID System
Office of the System Administrator OSA- responsible for protecting the integrity and performance of the AGDIS

Reportable incident investigation and oversight

Currently, entities participating in the Australian Government Digital ID System (including those whose approval is suspended or revoked) are required to notify the System Administrator of any cyber security or digital ID fraud incidents that occur or are reasonably suspected to have occurred in relation to accredited services.

The proposed amendments empower the System Administrator to direct entities that have made a notification to conduct an investigation into the incident. Broadly, the entities receiving such a direction must begin the investigation as soon as reasonably practicable, keep the System Administrator appraised and provide a summary of their findings once complete.

The proposed amendments ensure that investigations are actively monitored and progressed in a timely manner, improving coordination across the system. They strengthen oversight and accountability, helping ensure that incidents are investigated promptly and thoroughly, and reinforcing trust in the system's ability to respond to emerging risks.

Relying party machinery of government changes

The proposed amendments reduce the number of mandatory considerations or requirements for approval to participate in the Australian Government Digital ID System, in circumstances where a Commonwealth, state or territory government relying party will be providing a previously approved service, due to a machinery of government change.

A machinery of government change is when the structure or responsibilities of government departments and agencies are changed, for example, when functions are transferred between departments or agencies. These changes are common in public administration and aim to improve efficiency or align functions with government priorities.

Digital ID Data Standards Chair Trustmark authorisation

The Digital ID Rules authorise the Digital ID Regulator, System Administrator, Information Commissioner, and Secretary of the Department of Finance to use and display the digital ID trustmark.

The proposed amendment adds the Digital ID Data Standards Chair (**Data Standards Chair**) to the list of entities authorised to use and display the trustmark.

Consultation questions for other proposed changes:

Do the proposed changes promote the efficient and effective operation of the Australian Government Digital ID System?

Proposed changes to the Accreditation Rules

This section details the proposed changes contained in the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025* (**Accreditation Amendment Rules**).

The Accreditation Amendment Rules amend the Accreditation Rules to:

1. Revise the compliance model for the Protective Security Policy Framework (**PSPF**).
2. Provide an alternative period for the expiry of express consent given by an individual in relation to their use of an accredited Attribute Service Provider's accredited services for a business purpose.
3. Extend time within which certain accredited Identity Service Providers must enable individuals to request the suspension or resumption of their digital ID until 30 November 2026.

Protective Security Policy Framework updates

The PSPF sets out the protective security policy of the Australian Government.

Currently, under the Accreditation Rules, any accredited entity can choose between options including the Australian Government's PSPF as their digital ID protective security framework. The proposed amendments limit the option to use the PSPF to certain non-corporate Commonwealth entities (**NCEs**) under the *Public Governance, Performance and Accountability Act 2013* (**PGPA Act**). All other entities retain the option to implement the international standard ISO/IEC 27001 Information Security Management Systems or an alternative protective security framework as the basis for their accreditation.

The purpose of this change is to enhance alignment with whole-of-government protective security policy by mandating that NCEs comply with the PSPF, consistent with their obligations under the PGPA Act. This amendment improves regulatory precision by requiring compliance with specific PSPF controls, rather than the broader implementation of an entire framework as was previously the case.

Under the proposed amendments, entities using the PSPF must comply with the latest PSPF requirements. A 3 month transition period will apply following any future updates, providing entities sufficient time to implement changes. By incorporating the PSPF by reference, the Accreditation Rules will automatically reflect future updates to the PSPF as they take effect. This significantly simplifies the legislative framework by removing the need to replicate PSPF requirements within the Rules each time that the PSPF is updated. It also improves regulatory

responsiveness and ensures that entities are subject to the latest protective security controls. This change strengthens consistency between the PSPF and the Accreditation Rules.

Express consent expiry period

Currently, an individual's express consent given to any accredited entity for the collection, use or disclosure of their personal information, can be relied upon for a maximum of 12 months.

The proposed amendment creates a separate expiry period of 7 years when the individual declares that they are using an Attribute Service Provider's accredited services for or on behalf of a business (including a business they personally operate). This improves the user experience and reduces the regulatory impact of consent renewals on businesses. The 7 year period aligns with a comparable consent timeframe under the Consumer Data Right. Despite the change to the maximum period, an individual would still be able to withdraw consent at any time.

In the context of personal use, a 12 month limit is appropriate to ensure that consent remains valid and informed through regular renewal. By contrast, businesses often operate under contractual and internal governance frameworks that support long term or ongoing relationships with individuals acting on their behalf. Requiring authorised representatives and agents to renew their express consent every 12 months in these circumstances creates an unnecessary administrative and regulatory burden and may impact business productivity and services.

The 7 year consent timeframe applies to accredited Attribute Service Providers only**.** Currently, the only accredited Attribute Service Provider is the Australian Tax Office (**ATO**), which provides a service known as the Relationship Authorisation Manager (**RAM**). The RAM is used to link an individual's Digital ID (myID) to the Australian Business Number of the business or other organisation that the individual is authorised to represent.

The 12 month maximum expiry for express consent when acting in a personal capacity remains under the Accreditation Rules.

Practical example

- *Kim* owns a business. She uses the ATO's RAM to link her Digital ID to her business's Australian Business Number. She provides **express consent** to disclose her information to relying parties as part of linking her business.
- Kim authorises her employee, *Andy*, to act on behalf of her business with the ATO. Andy provides **express consent** to disclose his information to relying parties they have been granted access to act on behalf of the Australian Business Number, including ATO Online Services.

Under the current rules:

- Kim and Andy need to provide consent every 12 months to enable the RAM to disclose their information.
- Kim needs to do this for every business she owns.
- Both Kim and Andy can vary and revoke their consent at any time. Kim can revoke Andy's authorisation at any time.

After the proposed amendment:

- Kim and Andy can provide consent for up to 7 years to enable RAM to use and disclose their information.
- Both Kim and Andy can vary and revoke their consent at any time. Kim can revoke Andy's authorisation at any time.

Suspension and resumption of individual digital IDs

Under the Accreditation Rules, a Digital ID suspension may be initiated either by an Identity Service Provider in response to suspected fraud or cyber security incidents, or at the request of an individual for any reason.

The Accreditation Rules require Identity Service Providers to take specific steps if an individual requests a temporary suspension of their digital ID. The steps include confirmation that the request is genuine, suspension of the digital ID, and notification to the person that the digital ID has been suspended. Identity Service Providers are also required to follow steps to safely restore the digital ID after suspension.

The suspension and resumption provisions are scheduled to apply to *transitioned accredited entities* 12 months after the rules commenced. A transitioned accredited entity is an entity that was deemed to be accredited immediately after commencement of the Digital ID Act.

The proposed amendment delays the application of the suspension and resumption provisions for an additional 12 months, until 30 November 2026. This allows entities time to develop the necessary systems and processes to comply with the obligations.

Consultation questions for proposed changes:

Do the proposed changes promote the efficient and effective operation of the Accreditation Scheme?